

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-286904

(43) 公開日 平成8年(1996)11月1日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 A
	12/14	3 2 0		12/14 3 2 0 B
G 0 9 C 1/00	6 1 0	7259-5 J	G 0 9 C 1/00	6 1 0 Z
	6 6 0	7259-5 J		6 6 0 D

審査請求 未請求 請求項の数 9 O L (全 11 頁)

(21) 出願番号 特願平8-25674

(22) 出願日 平成8年(1996)2月13日

(31) 優先権主張番号 特願平7-25707

(32) 優先日 平7(1995)2月14日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72) 発明者 吉岡 誠

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

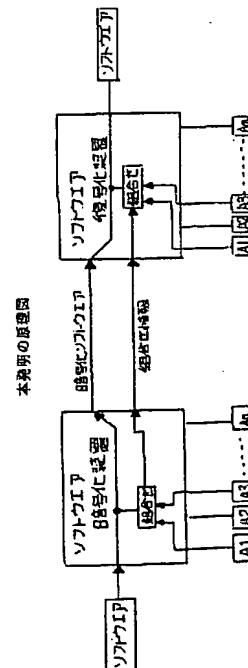
(74) 代理人 弁理士 遠山 勉 (外1名)

(54) 【発明の名称】 ソフトウェア暗号化・復号化方法、ソフトウェア暗号化システムおよびソフトウェア復号化システム

(57) 【要約】

【課題】 暗号化ソフトウェアの不正解読を簡易な技術で防止する

【解決手段】 ソフトウェアを暗号化する際に、2以上の暗号化基本アルゴリズムを採用するようにした。一方、ソフトウェア復号化処理ではこの2以上の暗号化基本アルゴリズムに対応した復号アルゴリズムを用意した。そして、ソフトウェア暗号化処理では暗号化ソフトウェアとともに暗号化した基本アルゴリズムの組合せ情報をソフトウェア復号処理に引き渡す。ソフトウェア復号処理では、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する逆アルゴリズムを選択して前記暗号化ソフトウェアを復号化するようにした。



【特許請求の範囲】

【請求項 1】 2 以上の暗号化基本アルゴリズムを組み合わせてソフトウェアを暗号化するソフトウェア暗号化ステップと、

暗号化されたソフトウェアを入力して前記暗号化に用いられた前記 2 以上の暗号化基本アルゴリズムの復号化アルゴリズムによって前記ソフトウェアを復号化するソフトウェア復号化ステップとからなり、

前記ソフトウェア暗号化処理は、暗号化ソフトウェアを生成するとともにこの暗号化ソフトウェアと 2 以上の基本アルゴリズムの組合せ情報を前記ソフトウェア復号化処理に引き渡す処理を含み、

前記ソフトウェア復号化処理は、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する復号化アルゴリズムを選択して前記暗号化ソフトウェアを復号化する処理を含むソフトウェア暗号化・復号化方法。

【請求項 2】 前記ソフトウェア復号化ステップは、前記基本アルゴリズムの組合せ情報と前記アルゴリズムに対する鍵情報とで前記暗号化ソフトウェアの復号化する処理を含む請求項 1 記載のソフトウェア暗号化・復号化方法。

【請求項 3】 ソフトウェアを提供するソフトウェア提供手段と、

2 以上の基本アルゴリズムを提供するアルゴリズム提供手段と、

前記アルゴリズム提供手段に提供された基本アルゴリズムの中から少なくとも 2 以上の基本アルゴリズムを選択する選択手段と、

前記ソフトウェア提供手段から読み出したソフトウェアを、選択手段によって選択結合された 2 以上の基本アルゴリズムで暗号化する暗号化実行手段と、

暗号化実行手段から出力された暗号化ソフトウェアを出力する出力手段とからなるソフトウェア暗号化システム。

【請求項 4】 請求項 3 のソフトウェア暗号化システムは、前記選択手段により選択された 2 以上の基本アルゴリズムの結合順序を記録する結合順序記録手段を有しており、

前記出力手段は、暗号化ソフトウェアとともに前記結合順序記録手段から得られた結合順序データを出力する請求項 3 記載のソフトウェア暗号化システム。

【請求項 5】 前記暗号化実行手段は、読み出したソフトウェアを特定のビット数毎の所定数のビット群に分割して前記ビット群のそれぞれに対して並行に前記選択手段で選択結合された 2 以上の基本アルゴリズムで暗号化処理を行い、暗号化された前記ビット群を結合する請求項 3 記載のソフトウェア暗号化装置。

【請求項 6】 前記暗号化実行手段は、読み出したソフトウェアを特定のビット数毎の所定数のビット群に分解して前記ビット群のそれぞれに対して順番に前記選択手

段で選択結合された 2 以上の基本アルゴリズムで暗号化処理を行い、暗号化された前記ビット群を結合する請求項 3 記載のソフトウェア暗号化装置。

【請求項 7】 暗号化されたソフトウェアを提供する暗号化ソフトウェア提供手段と、

2 以上の基本アルゴリズムを提供するアルゴリズム提供手段と、

前記アルゴリズム提供手段に提供された基本アルゴリズムの中からソフトウェアの復号に必要な特定の 2 以上の基本アルゴリズムを選択する選択手段と、

前記選択手段により選択された 2 以上の基本アルゴリズムの結合順序を記録する結合順序記録手段と、

前記暗号化ソフトウェア提供手段から提供された暗号化ソフトウェアを、選択手段によって選択結合された 2 以上の基本アルゴリズムで復号化する復号化実行手段とからなるソフトウェア復号化システム。

【請求項 8】 前記アルゴリズム提供手段は、2 以上の基本アルゴリズムを実行プログラム化して外部から物理的に保護された記録媒体内に保持されたものである請求項 7 記載のソフトウェア復号システム。

【請求項 9】 前記アルゴリズムの組合せ情報は更新可能であり、このアルゴリズムの組合せ情報は旧版の 2 以上の基本アルゴリズムの組み合わせによって暗号化されて更新組合せ情報として前記ソフトウェア復号化処理に引き渡されることを特徴とする請求項 1 記載のソフトウェア暗号化・復号化方法。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】本発明は、文字、音声、動画像、静止画またはプログラム等のデータを暗号化する技術、および暗号化されたこれらのデータを復号化する技術に関する。

【0002】

【従来の技術】ソフトウェアの流通形態として、文字、音声、動画像、静止画またはプログラム等のデータを暗号化してフロッピーディスク、CD-ROMやMO等の媒体に格納して販売する方式や、前記データを暗号化して通信回線を通じてユーザーに配信する方式等が採用されている。

【0003】このような従来の暗号化方式では、提供者（プロバイダー）はたとえばプログラムを単一のアルゴリズムで暗号化してユーザーに提供し、ユーザーはこれを前記プロバイダーから提供された「鍵」と呼ばれる暗号処理ソフトウェアで復号する作業を行っている。

【0004】しかしながら、ユーザー側にある暗号処理ソフトウェアは不正ユーザーにより解読されると、この解読結果に基づくコピーツールが作成されてしまう恐れがあり、このようなコピーツールが大量に出回ることによりプロバイダーは大きな損失を被ることにともなりかねない。

【0005】

【課題を解決するための手段】本発明は、このような問題に鑑みてなされたものであり、この種のソフトウェアが短期的にバージョンアップされる特性に着目して、暗号化のアルゴリズムをバージョンアップ毎または定期的に変更可能な暗号化組合せ方式を提供することにある。

【0006】本発明は、ソフトウェアを暗号化する際に、2以上の暗号化基本アルゴリズムを採用するようにした。ここで暗号化基本アルゴリズムとは、入力データ列を攪乱するために必要な最低限の処理をいう。この処理はたとえば入力データ列を組み替えること、置き換えること、または他の乱数列との排他的論理和をとること等を意味している。

【0007】一方、ソフトウェア復号化処理（ソフトウェア暗号化装置）ではこの2以上の暗号化基本アルゴリズムに対応した復号アルゴリズムを用意した。そして、ソフトウェア暗号化装置は暗号化ソフトウェアとともに暗号化したアルゴリズムの組合せ情報をソフトウェア復号手段（ソフトウェア復号化装置）に引き渡す。

【0008】ソフトウェア復号手段は、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する復号アルゴリズムを選択して前記暗号化ソフトウェアを復号化するようにした。

【0009】前記した手段において、ソフトウェアは暗号化装置に入力されると、任意のアルゴリズムの組合せ（たとえばA1およびA3）によって暗号化される。このように暗号化されたソフトウェアは、CD-ROMあるいは通信回線を通じて流通されてユーザーに届く。ユーザーは自身が保有する復号装置においてこの暗号化ソフトウェアを復号化するが、このときユーザーは暗号化装置で用いた暗号の組合せ情報（たとえばA1 | A3）に基づいて当該暗号化ソフトウェアを復号する。この組合せ情報は暗号化ソフトウェアとともに同一媒体でユーザーのもとに到着するようにしてもよいし、あるいは別媒体または図示しない鍵情報「K」とともにユーザーに伝えられるようにしてもよい。また、この組合せ情報は、更新前のアルゴリズムを用いて暗号化してもよい。

【0010】このようにすれば、たとえば個々では解析容易な程度の低い基本アルゴリズムであっても組み合わせさせて暗号化することにより解析の困難性を高めることができる。このことは、たとえば個々の基本アルゴリズムは容易に把握可能なものであっても、この基本アルゴリズムの組合せは膨大な数にのぼるため、この組合せそのものを解析するには多大な労力と時間が必要となり、事実上解析が困難になる。また、仮に解析が可能になったとしても、ソフトウェアのバージョンアップによってさらにアルゴリズムの新しい組合せでソフトウェアが暗号化されるため、最近の短期なサイクルでのソフトウェアのバージョンアップに十分に対応できる。

【0011】したがって、この暗号化ソフトに挑戦するためにハッカーは無数の組合せの暗号アルゴリズムに直面しなくてはならず、事実上解読作業を断念せざるを得なくなる。

【0012】

【発明の実施の形態】以下、図面に基づいて、本発明の実施の形態を説明する。図1に示すように、本発明では、ソフトウェアを暗号化する際に、2以上の暗号化基本アルゴリズムを採用するようにした。一方、ソフトウェア復号化処理（ソフトウェア暗号化装置）ではこの2以上の暗号化基本アルゴリズムに対応した復号アルゴリズムを用意した。そして、ソフトウェア暗号化装置は暗号化ソフトウェアとともに暗号化した基本アルゴリズムの組合せ情報をソフトウェア復号手段（ソフトウェア復号化装置）に引き渡す。

【0013】ソフトウェア復号手段は、前記基本アルゴリズムの組合せ情報に基づいて自身の保有する復号アルゴリズムを選択して前記暗号化ソフトウェアを復号化するようにした。

【0014】これにより、ソフトウェアは暗号化装置に入力されると、任意の基本アルゴリズムの組合せ（たとえばA1およびA3）によって暗号化される。このように暗号化されたソフトウェアは、CD-ROMあるいは通信回線を通じて流通されてユーザーに届く。ユーザーは自身が保有する復号装置においてこの暗号化ソフトウェアを復号化するが、このときユーザーは暗号化装置で用いた暗号の組合せ情報（たとえばA1 | A3）に基づいて当該暗号化ソフトウェアを復号する。この組合せ情報は暗号化ソフトウェアとともに同一媒体でユーザーの元に到着するようにしてもよいし、あるいは別媒体または図示しない鍵情報「K」とともにユーザーに伝えられるようにしてもよい。

【0015】図2および図13は、本発明の実施例であるソフトウェア暗号化装置のハードウェア構成を示している。コンピュータ本体（BDY）にはICカードスロット（ICR）とフロッピーディスクドライブ（FD）が設けられている。また図には示していないがコンピュータ本体（BDY）にはモデム（MDM）や受信装置が内蔵されており、有線または無線経路を通じて外部とデータの送受信が可能である。

【0016】コンピュータ本体（BDY）には入力装置としてキーボード（KEY）およびマウス（MOU）が接続されている。またコンピュータ本体（BDY）には出力装置としてディスプレイ（CRT）およびプリンタ（PRN）が接続されている。

【0017】コンピュータ本体（BDY）にはさらに外部記憶装置として光ディスクドライブ装置（MOD）が接続されている。またコンピュータ本体（BDY）内にはハードディスク装置が内蔵されている。

【0018】図2において、BUSはバスであり、制御

バスおよびデータバスを意味している。CPUは中央制御部であり、32ビットまたは64ビット処理のプロセッサが用いられている。MEMはメモリであり、後述の暗号組合せテーブルや作業領域が特定のアドレスによって設定される。

【0019】ソフトウェア提供手段としてはフロッピーディスクのみを図示しているが、これに限らず、光磁気ディスクあるいは通信回線であってもよい。さらに、メモリMEMあるいは中央制御部CPU内のバッファもソフトウェア提供手段として機能する。

【0020】ICRはICカードリーダーであり、JEIDA準拠のPCMCIAカードを装着することが可能である。本実施例において後述のアルゴリズムプログラムA1、A2、A3・・・AnはこのICカードに格納されて提供される。このICカードには物理的なプロテクトを施すことが好ましく、たとえば、ユーザーの不正な開封によってアルゴリズムのデータを消滅させたり、読み出しを禁止するようにしてもよい。さらにこのICカードは所定の期間毎にその複数のアルゴリズムの構成を変更してもよい。一定期間毎にICカード内に格納されるアルゴリズムの配置または内容を更新できるようにすれば、ソフトウェアの復号を期間的に限定させることができ、デモソフトあるいは使用に応じた従量制ソフトウェアに対応することができる。

【0021】MODは光磁気ディスク装置であり、100メガバイト以上の容量を有する光磁気ディスク媒体の読み書きが可能となっている。また、IFは通信インターフェースであり、外部の通信回線と接続されている。

【0022】なお、以上の装置構成の他に、たとえばCD-ROMスタンピング装置を接続してもよい。以上図2はソフトウェア暗号化装置として説明したが、これに対応したソフトウェア復号化装置も同様の構成を有している。ただし、当該装置をソフトウェア復号化装置として用いる場合には、CD-ROMドライブを設けてもよい。すなわち、音声、静止画、動画像等の大量データを流通させる媒体としてはCD-ROMが適しているためである。

【0023】図3は、本実施例のシステム構成を機能ブロックで表したものである。同図において上段はソフトウェア暗号化装置の機能を示しており、下段はソフトウェア復号化装置の機能を示している。

【0024】図3の機能と図2で説明したハードウェアとの関係を説明すると、図3におけるアルゴリズムプログラム(A1、A2・・・An)はICカードに格納されて提供されている。また選択処理、結合処理、結合プログラム処理は中央制御部(CPU)によって実現される機能である。鍵情報「K」はキーボード(KEY)より入力される。また、ソフトウェア格納ファイルはフロッピーディスク装置(FD)または光磁気ディスク装置(MOD)を通じて入力されてメモリ(MEM)上に

読み込まれる。

【0025】次に、図3を用いてソフトウェアの暗号化処理について説明する。まず、中央制御部(CPU)の選択処理によりソフトウェアの暗号化処理に用いられるアルゴリズムを決定する。ここでは2以上の基本アルゴリズムプログラムを決定する処理が行われる。基本アルゴリズムの決定は、たとえばメモリ(MEM)上に設定される図4に示すようなアルゴリズムテーブルを用いてもよい。

10 【0026】アルゴリズムテーブルには同図に示すように、A1、A2・・・Anのn個の基本アルゴリズムが行列状に設定されている。このようにn個の基本要素(アルゴリズム)から重複を許可して2個の結合アルゴリズムを用いる場合nの2乗の結合アルゴリズムを生成できる。

20 【0027】一方、n個の基本要素(アルゴリズム)から任意の個数をタンデム接続してその組合せを考えた場合、各要素(アルゴリズム)の並び替えを行った場合、最大n!個の結合アルゴリズムを得ることができる。さらに、重複並び替えを許可した場合、最大nのn乗の個数の結合アルゴリズムを生成できる。

【0028】たとえばアルゴリズムA1とA2とを組み合わせるとA1|A2とすることもできるし、3個のアルゴリズムの組合せによってたとえばA1|A2|A3とすることもできる。また同一のアルゴリズムをL段組み合わせるとたとえばA1|A1|A1|・・・|A1としてもよい。

30 【0029】このように本実施例では基本アルゴリズムの組合せが多数生成できるため、たとえば個々の基本アルゴリズムとしては解析容易であっても組合せ結合によって解析困難なアルゴリズムとして用いることができる。

【0030】次に、具体的なアルゴリズムの例について説明する。図5は、転置型基本アルゴリズムの具体例を示している。すなわち、本アルゴリズムでは鍵連動交換スイッチがプログラムとして設定されており、8ビットのデータ毎にビット位置が入れ替えられて出力されるようになっている。入れ替え位置を制御するのが外部から与えられる鍵情報「K」である。なお同図では入出力を8ビット構成としているが、これに限定されない。このような転置型基本アルゴリズムはたとえば前述のアルゴリズムテーブルに「A1」として登録されている。

【0031】図6は、換字型基本アルゴリズムの具体例を示している。このアルゴリズムでは入力データに対して出力するデータをテーブル化して保有している。なお同図では入出力を3ビット構成としているがこれに限られないことはいうまでもない。このような換字型基本アルゴリズムはたとえば前述のアルゴリズムテーブルに「A2」として登録されている。

50 【0032】図7は、排他アルゴリズムの具体例を示し

ている。本アルゴリズムでは、たとえば入力された各ビットに対して鍵情報「K」を用いて排他論理処理を行う。なお同図では入出力を3ビット構成としているがこれに限られないことはいうまでもない。このような排他アルゴリズムはたとえば前述のアルゴリズムテーブルに「A3」として登録されている。

【0033】図8は、乗算型基本アルゴリズムの具体例を示している。この図では8ビットのデータが入力されると、鍵情報「K」によって乗算器で当該入力データが乗算された後、出力マスキング回路によってマスクされたデータが出力される。このような乗算型アルゴリズムはたとえば前述のアルゴリズムテーブルに「A4」として登録されている。

【0034】以上のような複数のアルゴリズムからアルゴリズムが中央制御部（CPU）の「選択処理」により選択されると、結合処理（暗号化実行手段）が行われる。この結合処理の具体例を示したものが図9および図10である。

【0035】図9はDES型結合の一例を示したものである。同図において、ソフトウェアデータが入力されると、これを所定のビット毎（たとえば8ビット毎）に分割して処理を行う。ここでは、前記8ビット中の上位4ビットを左半分データ（D1）、下位4ビットを右半分データ（D2）に分割する。

【0036】そして、右半分データ（D2）はA1アルゴリズムによって処理され暗号化データC1として出力される。左半分データ（D1）は、前記暗号化データ（C1）と排他論理処理されて暗号化データ（D1+C1）として出力される。

【0037】一方、左半分データ（D1）とA1アルゴリズムの出力データ（C1）の排他論理処理出力データは、A2アルゴリズムで処理されて暗号化データC2として出力される。この暗号化データC2は、右半分データ（D2）と排他論理処理されて、暗号化データ（D2+C2）として出力される。

【0038】なお、図9の復号処理については図は省略するが、図9の「A1プログラム」（A1の復号アルゴリズム）と「A2プログラム」（A2の復号アルゴリズム）を入れ替えたシステムを用意すればよい。

【0039】図10は、ENIGMA結合の一例を示したものである。この例では入力されたソフトウェアをA1アルゴリズムで一次変換した後、A2プログラムで二次変換する

また同図左半部に示しているように、これを復号化する場合には、まずアルゴリズムA2の復号アルゴリズムA2⁻¹にて一次復号を行った後、アルゴリズムA1の復号アルゴリズムA1⁻¹にて二次復号を行うことによって元のソフトウェアに戻すことができる。

【0040】次に図11を用いて、アルゴリズムとして転置型アルゴリズム（A1）と換字型アルゴリズム（A

2）を結合してENIGMA型結合処理を行う場合についてさらに具体的な実例によって説明する。

【0041】まず、鍵連動交換スイッチに対して鍵情報「K」が与えられる。この鍵情報「K」は入力される8ビットデータに対して出力をどのビットに転置するかを規定した情報である。同図では第1ビット→第7ビット、第2ビット→第3ビット、第3ビット→第2ビット、第4ビット→第5ビット、第5ビット→第1ビット、第6ビット→第8ビット、第7ビット→第6ビット、第8ビット→第4ビットに設定された鍵情報「K」が鍵連動交換スイッチに与えられている。

【0042】ここで、ソフトウェアデータ（平文データ）として「0Fh」、すなわち「00001111」が与えられると、前述の鍵情報「K」により規定された鍵連動交換スイッチにより第1ビットの「0」は第7ビットへ、第2ビットの「0」は第3ビットへ、第3ビットの「0」は第2ビットへ、第4ビットの「0」は第5ビットへ、第5ビットの「1」は第1ビットへ、第6ビットの「1」は第8ビットへ、第7ビットの「1」は第6ビットへ、第8ビットの「1」は第4ビットへそれぞれ転置される。この結果、アルゴリズムA1による変換結果は「10010101」すなわち「95h」となる。

【0043】次にアルゴリズムA1によって一次暗号化されたデータ「95h」を換字型アルゴリズムA2によって二次暗号化する。ここではまず、入力データ（95h）を上位4ビットの左半分データと、下位4ビットの右半分データとに分割してそれぞれの変換テーブルに基づいて変換を行う。この結果、二次暗号化出力データは「00100000」すなわち「20h」となる。

【0044】次に、図3に示すように、以上の選択処理、結合処理および結合プログラム処理が行われて暗号ソフトウェアが生成されると、この暗号ソフトウェアはMO、CD-ROM、フロッピーディスク等の媒体に格納されて提供者よりユーザーに配送される。また、インターフェース（I/O）を通じて通信回線を経由してユーザーのもとに配信されるようにしてもよい。またこのとき、アルゴリズムの選択順番コード、たとえば前述の例では「A1||A2」というコードがMO、CD-ROM、フロッピーディスク等の媒体に暗号化ソフトウェアとともに格納される。また通信による場合は暗号化ソフトウェアとともに通信路に送出される。

【0045】なお、この選択順番コードは前記暗号化ソフトウェアとは別の配信経路、たとえば電話による口頭説明等で提供者よりユーザーに伝えられてもよい。さらに鍵情報「K」とともに選択順番コードをユーザーに提供してもよい。

【0046】前記暗号化ソフトウェアと選択順番コードを受信したユーザー側の復号化装置では、前記選択順番コードの情報に基づいて復号アルゴリズムを選択して結

合処理および結合プログラム処理を行って復号化ソフトウェアを得る。

【0047】この復号処理の具体例を示したものが図12である。同図において、暗号化ソフトウェアより暗号化データが8ビットずつ(20h)入力されると、その上位4ビットと下位4ビットとをそれぞれ左半分データ、右半分データとしてアルゴリズムA2⁻¹による換字変換がまず実行される。この換字変換により得られた一次復号化データ(95h)は、さらに転置型アルゴリズムA1⁻¹による転置変換が行われ復号データとして「00001111」すなわち「0Fh」が得られる。

【0048】ところで、アルゴリズムの組合せ情報(図11の例ではA1||A2)と鍵情報「K」とが一旦外部に漏洩されてしまうと暗号化ソフトウェアの解読は極めて容易になってしまう。そこで、たとえば組合せ情報と鍵情報に対してさらに2以上の基本アルゴリズムを組み合わせて暗号化し、これを復号化情報として提供者からユーザーに伝える。

【0049】これを受け取ったユーザーは初期鍵によってこの暗号化された復号化情報を復号して前記暗号化ソフトウェアの復号に必要な組合せ情報と鍵情報とを得る。前記復号化情報は定期的に更新され、新たな復号化情報は、旧版の復号化情報中の組合せ情報を用いて生成される。

【0050】したがって、ユーザーは復号化情報を復号するためには常に一世代前の直近の復号化情報中の組合せ情報が必要になる。これにより、いずれかの時点での暗号化キー情報が外部に漏洩したとしても、一世代前の直近の暗号化キー情報を有していなければ暗号化ソフトウェアを解読(復号)することは困難になる。

【0051】

【発明の効果】本発明によれば、個々では解析容易な程度の低い基本アルゴリズムであっても組み合わせて暗号化することにより解析の困難性を高めることができる。このことは、たとえば個々の基本アルゴリズムは容易に把握可能なものであっても、この基本アルゴリズムの組

合せは膨大な数にのぼるため、この組合せそのものを解析するには多大な労力と時間が必要となり、事実上解析が困難になる。また、仮に解析が可能になったとしても、ソフトウェアのバージョンアップによってさらにアルゴリズムの新しい組合せでソフトウェアが暗号化されるため、最近の短期なサイクルでのソフトウェアのバージョンアップに十分に対応できる。

【図面の簡単な説明】

【図1】 本発明の原理図

【図2】 実施の形態のハードウェアの構成図

【図3】 実施の形態のシステム構成の機能ブロック図

【図4】 実施の形態のアルゴリズムテーブルを示す説明図

【図5】 転置型アルゴリズムの具体例を示す説明図

【図6】 換字型アルゴリズムの具体例を示す説明図

【図7】 排他アルゴリズムの具体例を示す説明図

【図8】 乗算型アルゴリズムの具体例を示す説明図

【図9】 DES型結合処理の具体例を示す説明図

【図10】 ENIGMA結合の具体例を示す説明図

【図11】 転置型アルゴリズム(A1)と換字型アルゴリズム(A2)を結合してENIGMA型結合処理を行う場合の具体例を示す説明図

【図12】 図11の結合処理で暗号化された暗号化ソフトウェアを復号化する場合の具体例を示す説明図

【図13】 実施の形態のハードウェア構成を示す説明図

【符号の説明】

CPU・・・中央制御部

KEY・・・キーボード

FD・・・フロッピーディスク装置

ICR・・・ICカードリーダー

MEM・・・メモリ

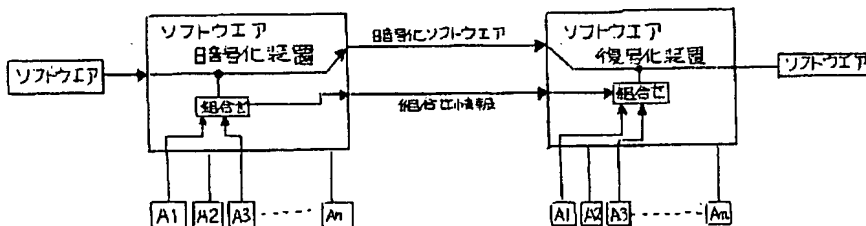
MOD・・・光磁気ディスク装置

MO・・・光磁気ディスク

I/F・・・通信インターフェース

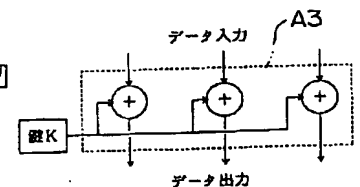
【図1】

本発明の原理図



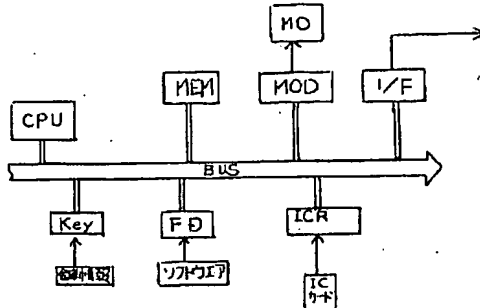
【図7】

排他アルゴリズムの具体例を示す説明図



【図 2】

実施例のハードウェアの構成図



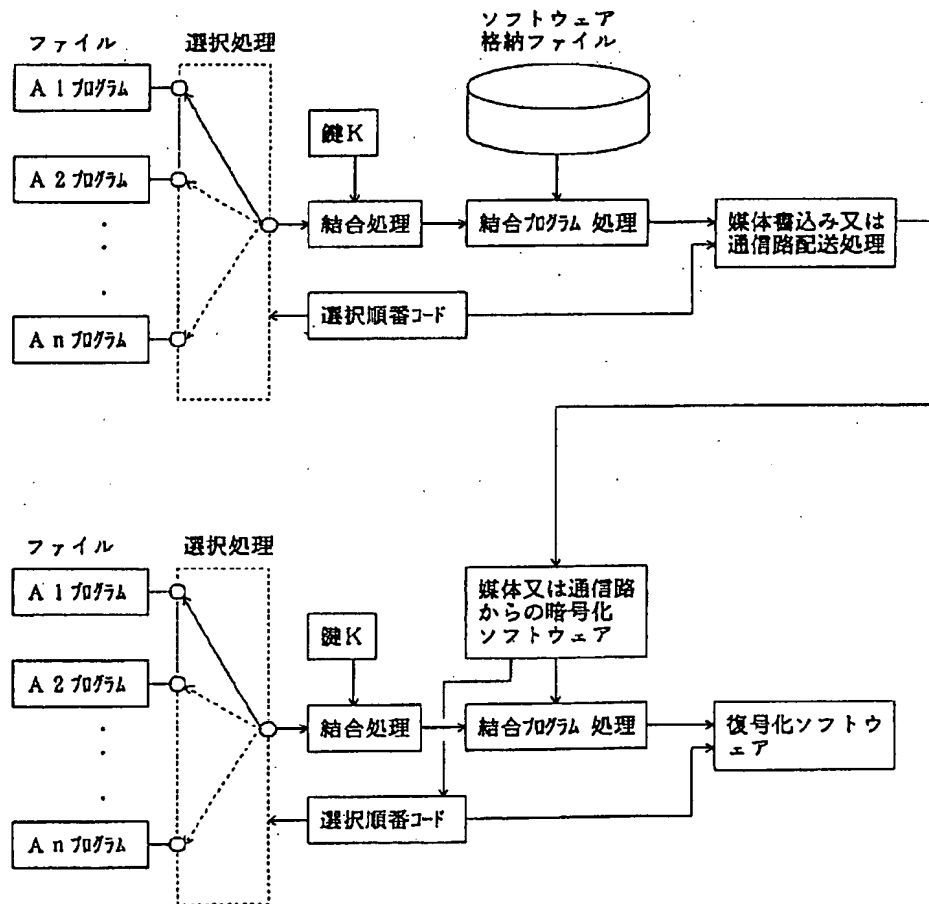
【図 4】

実施例のアルゴリズムテーブルを示す説明図

各種アルゴリズム					
	A 1	A 2	A n
A 1	A11	A12			A1n
A 2	A21	A22			A2n
...					
...					
...					
A n	An1	An2			Ann

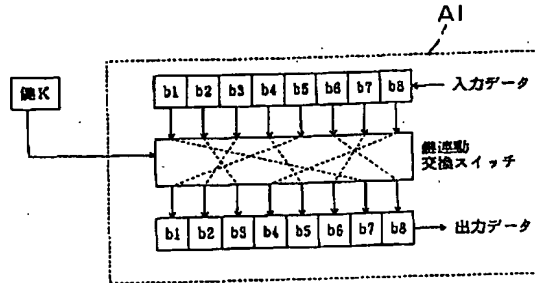
【図 3】

実施例のシステム構成の機能ブロック図



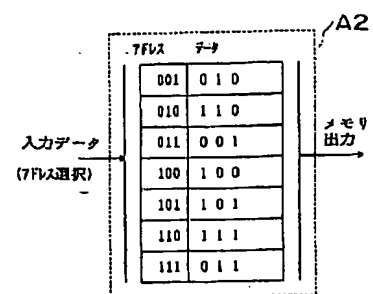
【図 5】

転置型アルゴリズムの具体例を示す説明図



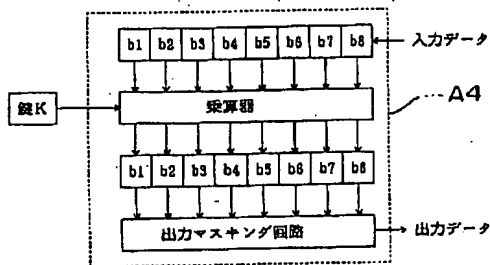
【図 6】

換字型アルゴリズムの具体例を示す説明図



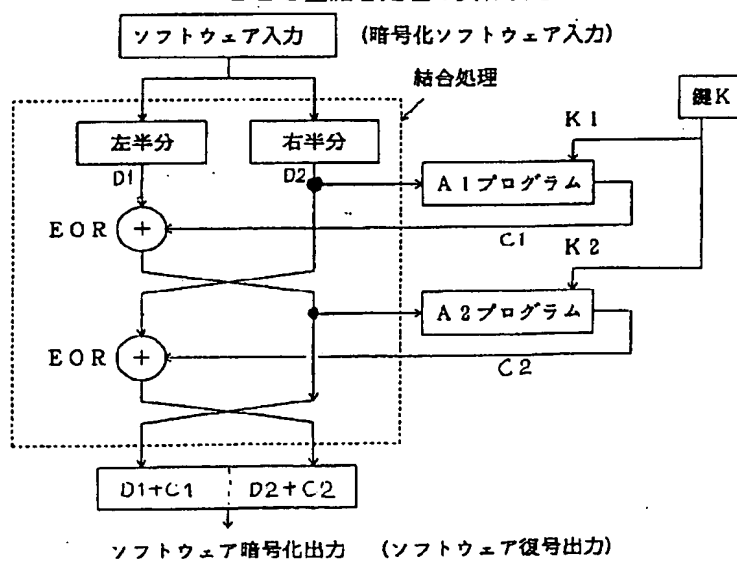
【図 8】

乗算型アルゴリズムの具体例を示す説明図

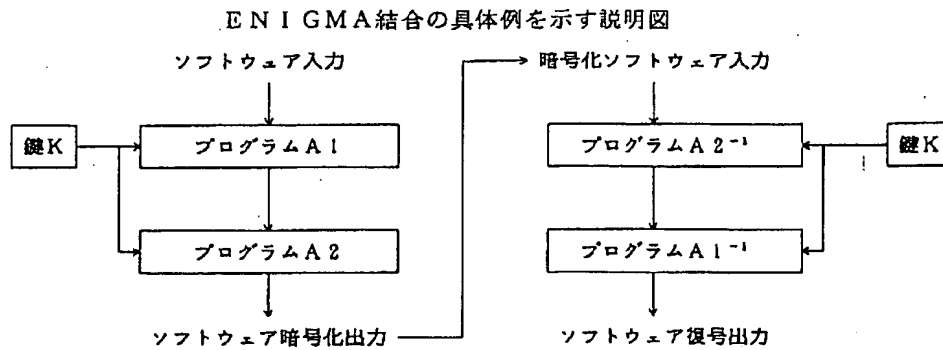


【図 9】

DES型結合処理の具体例を示す説明図

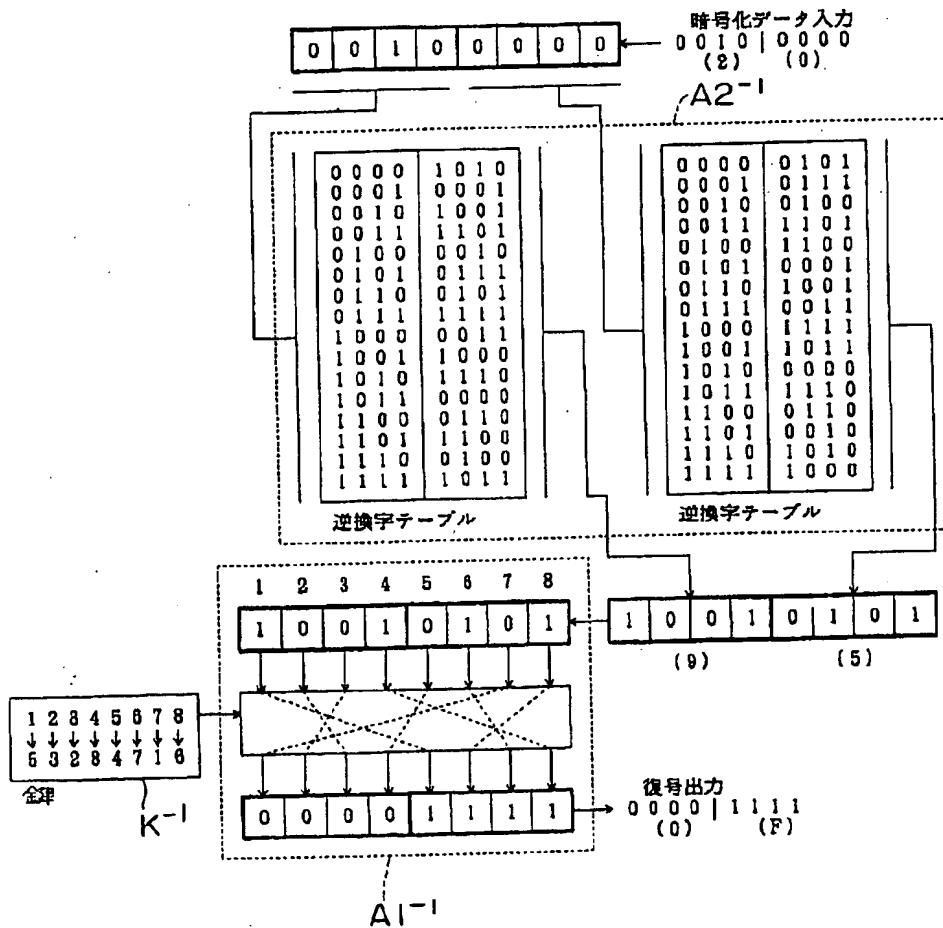


【図10】



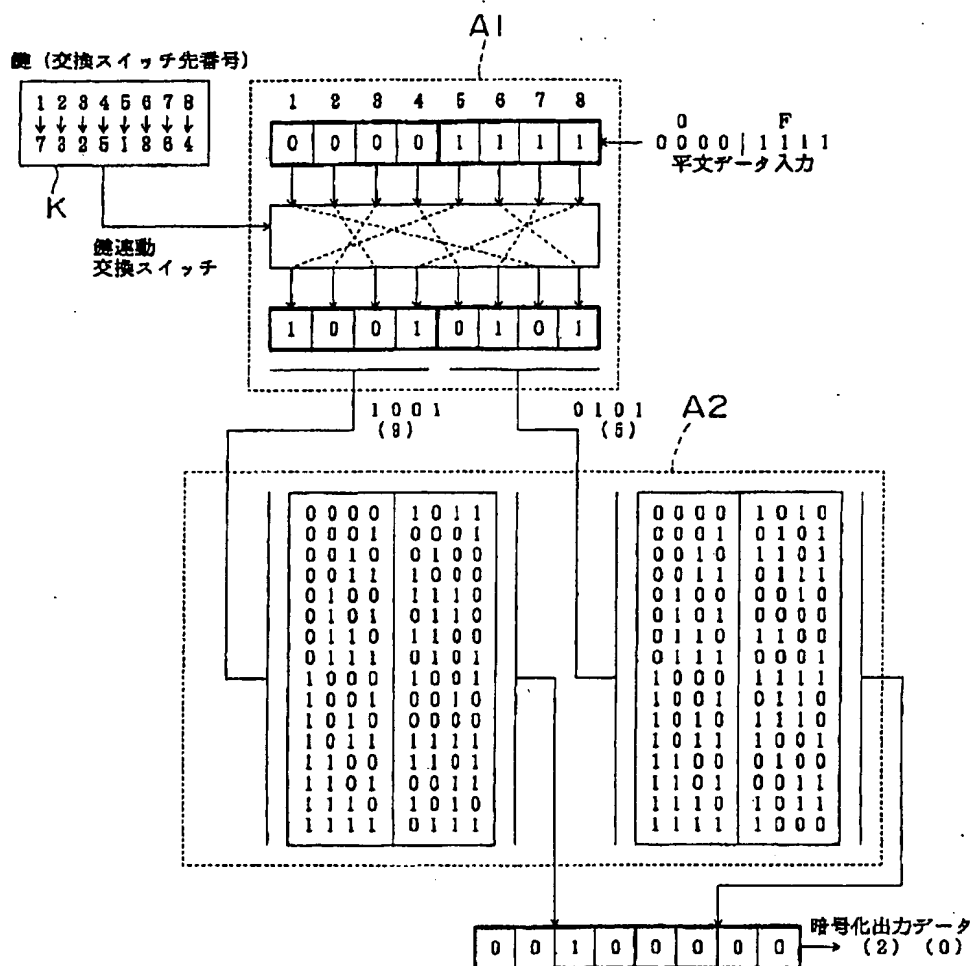
【図12】

図11の結合処理で暗号化された暗号化ソフトウェアを復号化する場合の具体例を示す説明図



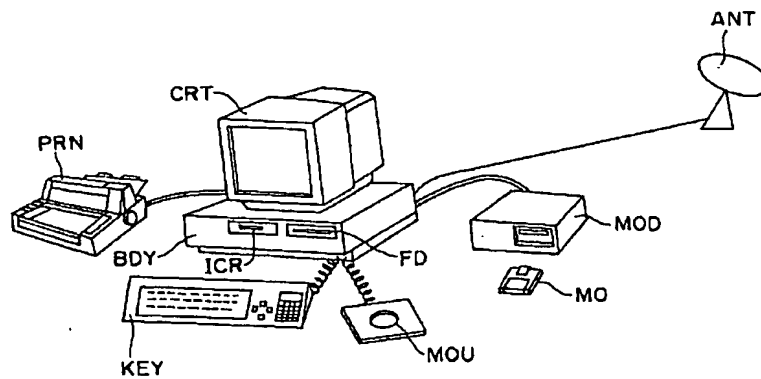
【図11】

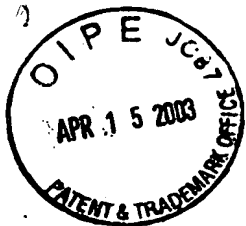
転置型アルゴリズム (A1) と換字型アルゴリズム (A2) を結合してENIGMA型結合処理を行う場合の具体例を示す説明図



【図13】

実施例のハードウェア構成を示す説明図





Japanese Patent Laid-open No. HEI 8-286904 A

Publication date : November 1, 1996

Applicant : Fujitsu Limited

Title : SOFTWARE ENCRYPTION AND DECODING METHOD, SOFTWARE

5 ENCRYPTION SYSTEM, AND SOFTWARE DECODING SYSTEM

RECEIVED
APR 18 2003
GROUP 3600

[ABSTRACT]

[Problem] To prevent the illegal decryption of encrypted software by simple technique.

10 [Solving Means] Not less than two encryption basic algorithms are used to encrypt a software. Decoding algorithms corresponding to the not less than two encryption basic algorithms are prepared, respectively, for a software decoding processing. In a software encryption processing, encrypted combination information on encryption basic algorithms as well as an encrypted software are transferred to a software
15 decoding processing. In the software decoding processing, inverse algorithms held by the unit are selected based on the basic algorithm combination information, and the encrypted software is decoded using the selected algorithms.

[Claim 1] A software encryption and decoding method comprising:

20 a software encryption step of encrypting a software using a combination of not less than two encryption basic algorithms; and

a software decoding step of inputting the encrypted software, and decoding the software based on decoding algorithms corresponding to the not less than two encryption basic algorithms used for encryption, wherein

25 in a software encryption processing, the encrypted software is generated, and

Best Available Copy

Best Available Copy

the encrypted software and combination information on the not less than two basic algorithms is transferred to a software decoding processing, and

in the software decoding processing, decoding algorithms held by a software decoding device are selected based on the combination information on the basic algorithms, and the encrypted software is thereby decoded.

[0012]

[MODE FOR CARRYING OUT THE INVENTION]

The embodiment of the present invention will be explained hereinafter with reference to the drawings. As shown in Fig. 1, the present invention adopts not less than two encryption basic algorithms to encrypt a software. Decoding algorithms corresponding to the encryption basic algorithms are prepared for a software decoding processing (software encryption device). The software encryption device transfers combination information on encrypted basic algorithms as well as an encrypted software to the software decoding unit (software decoding device).

[0013] The software decoding unit selects decoding algorithms held by the unit itself based on the basic algorithm combination information, and decodes the encrypted software.

[0014] By doing so, if a software is input to the encryption device, the software is encrypted based on an arbitrary basic algorithm combination (e.g., algorithms A1 and A3). The software thus encrypted arrives at a user through a CD-ROM or a communication line. The user decodes this encrypted software by the decoding device that the user owns. During decoding, the user decodes the encrypted software based on encryption combination information (e.g., A1 | A3) employed in the encryption device. This combination information may arrive at the user by the same

medium as that for the encrypted software or may be conveyed to the user by a different medium or as key information "K", not shown.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.